ANEXO VII

SEGURIDAD FÍSICA Y AMBIENTAL

1. OBJETIVO

Garantizar la adopción de las medidas necesarias para prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la S.R.T..

Proteger los activos físicos de procesamiento de información crítica, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, y controlando los factores ambientales que podrían perjudicar su correcto funcionamiento.

2. ALCANCE

Comprende todos los recursos físicos relativos a los sistemas de información de la S.R.T., como son edificios, instalaciones, equipamiento, cableado y medios de almacenamiento.

3. DEFINICIONES

Activos físicos de procesamiento de información crítica: equipos e instalaciones de procesamiento de aquella información que resulta indispensable para el correcto funcionamiento del Organismo y sus operaciones***.***

Área de recepción y distribución: espacio de acceso público en donde se reciben insumos, equipos y materiales en general por parte de terceros y se asigna su distribución dentro del Organismo.

Área segura: son sitios protegidos en los que se gestiona información sensible, donde se encuentra el equipamiento que procesa, almacena y transmite la información y el personal que los opera, así como zonas donde se encuentren resguardados los activos de información. En el contexto de la seguridad física, el término “sitio” significa edificios, recintos u oficinas que albergan todos los servicios e instalaciones.

Daños de origen ambiental: aquellos que puedan comprometer la información o procesamiento de la misma a partir de un incidente externo o interno relacionado con el entorno de trabajo, como inundaciones, incendios, etc.

Equipamiento informático: conjunto de dispositivos electrónicos (hardware) que permite la ejecución de programas informáticos (software) para el procesamiento de información

Infraestructura: edificios, equipamiento e instalaciones que soportan el desarrollo de las actividades de la organización.

Instalaciones y equipos con impacto en el procesamiento de información: se refiere al conjunto de equipos e instalaciones auxiliares y de soporte como por ejemplo UPS, generadores, instalación eléctrica, instalación contra incendios, etc., que garantizan las condiciones para el funcionamiento de los equipos de procesamiento de información crítica.

Materiales peligrosos: por su composición pueden ser explosivos, combustibles, tóxicos o corrosivos, pudiendo dañar tanto a las instalaciones, como a los equipos y personas.

Perímetro de Seguridad: área delimitada por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación, o un escritorio u oficina de recepción atendidos por personas.

UPS (Uninterruptable Power Supply por sus siglas en inglés): también llamado Sistema de Alimentación Ininterrumpida, es un dispositivo que permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) debe definir junto con la Subgerencia de Sistemas (S.S.) y los responsables de la información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos físicos críticos, en función a un análisis de riesgos sobre los mismos.

La S.S. colabora con el RSI en la definición de las medidas de seguridad a implementar en áreas seguras y coordina su implementación. Asimismo, debe asegurar el mantenimiento del equipamiento informático tanto dentro como fuera de las instalaciones.

Cuando sea requerido, los Titulares de las Unidades Organizativas serán quienes autoricen formalmente el trabajo fuera de las instalaciones al personal de la S.R.T. bajo su ámbito de competencia.

La Subgerencia de Infraestructura (S.I.) debe llevar a cabo la implementación de las medidas de seguridad establecidas por el RSI y la S.S. en las instalaciones de la S.R.T.. Asimismo, debe asegurar no sólo el mantenimiento del equipamiento de su competencia, sino también de los aspectos edilicios que involucren la seguridad física y ambiental.

Todo el personal de la S.R.T. es responsable del cumplimiento de las medidas adoptadas por el Organismo respecto a las pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario.

5. CONTENIDO

5.1 IDENTIFICACIÓN Y PROTECCIÓN DE ÁREAS SEGURAS

La función principal de la seguridad física es proteger los activos de información del acceso físico no autorizado, así como también evitar el daño e interferencia de la información de la S.R.T.. Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.

Asimismo, para la selección y el diseño de un área segura, se debe tener en cuenta la posibilidad de daño tanto físico o ambiental, generado por incendio, inundación, explosión u otras formas de desastres naturales o provocados por el hombre.

5.1.1 Perímetro de seguridad física

Se deberán definir y establecer perímetros de seguridad para proteger las áreas que contienen los activos de información. Asimismo, deberán establecerse medidas de seguridad adicionales en aquellos recintos donde se encuentren las instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

El emplazamiento y la fortaleza de cada barrera deberán ser definidos de acuerdo al análisis de riesgos efectuado oportunamente.

El acceso a las áreas seguras y edificios, deberán estar restringido exclusivamente al personal autorizado. Los métodos implementados registrarán e identificarán cada ingreso y egreso en forma precisa, con sus respectivos controles cronológicos.

Se emitirán lineamientos respecto de los controles y requerimientos necesarios en cuanto a la seguridad física en las sedes de la S.R.T. y las instalaciones de procesamiento de información, teniendo en cuenta los siguientes aspectos:

- Definir claramente el/los perímetro/s de seguridad;
- Ubicar las instalaciones de procesamiento de información dentro del perímetro de un área segura;
- Definir las barreras físicas necesarias para asegurar el perímetro de seguridad que corresponda a dicha área;
- Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se debe implementar medios alternativos de control de acceso físico al área o edificio que serán establecidos oportunamente;
- Definir y controlar áreas de recepción y distribución de equipamiento e insumos;
- Identificar claramente todas las puertas de emergencia de un perímetro de seguridad;
- Proponer el uso de mecanismos de control para la detección de personal no autorizado en las áreas seguras: cámaras, sensores de movimiento y cerrojos con tarjeta inteligente o control biométrico. Éstos se instalarán según estándares profesionales y, además, deberán ser probados periódicamente.

5.1.2 Protección contra amenazas y daños de origen ambiental

Se deberán, asimismo, identificar y proteger las áreas seguras contra daños de origen ambiental, considerando los siguientes aspectos para cada edificio de la S.R.T.:

- Su emplazamiento;
- Su ubicación geográfica y el entorno medioambiental;
- El entorno edilicio.

Adicionalmente, se deberá:

- Proporcionar equipo contra incendios ubicado adecuadamente;
- Almacenar materiales peligrosos o combustibles en lugares específicos definidos oportunamente, a una distancia prudencial de las áreas seguras que contienen activos de información considerados sensibles o críticos;
- No almacenar suministros como papelería en las áreas seguras que contienen activos de información considerados sensibles o críticos.

5.1.3 Áreas de recepción, retiro y depósito de equipamiento e insumos

Se deberán controlar las áreas de recepción, retiro y depósito de equipamiento e insumos. Para ello corresponderá contemplar controles físicos, de acuerdo a la disponibilidad y condiciones edilicias de cada sede de la S.R.T., incluyendo las Comisiones Médicas, conforme a los siguientes lineamientos:

- Diseñar las áreas de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio;
- Limitar el acceso a las áreas de depósito sólo al personal previamente identificado y autorizado;
- Registrar el material entrante y saliente al Organismo.

5.1.4 Control de acceso físico de ingreso y egreso

Las áreas seguras se deben resguardar mediante el empleo de controles de acceso físico, a fin de permitir que sea solo para el personal autorizado. Estos controles deben reunir las siguientes características:

- El uso de una identificación unívoca para todo el personal, con la finalidad de poder identificar y registrar cronológicamente el acceso a los edificios y áreas seguras;

- Controlar y limitar el acceso a las instalaciones de procesamiento de información clasificada como crítica exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación para autorizar y validar todos los accesos, como por ejemplo controles biométricos. listado de personas habilitadas y tarjeta inteligente o control biométrico;
- Supervisar o inspeccionar a los visitantes a los edificios y áreas seguras, y registrar la fecha y horario de su ingreso y egreso;
- Permitir el acceso mediando propósitos específicos y autorizados previamente.

5.1.5 Trabajo en áreas seguras

Para incrementar la seguridad de las áreas seguras, se deberán establecer controles y lineamientos, además de seguir los protocolos de seguridad e higiene vigentes en el Organismo, tanto para el personal que trabaja en dichas áreas, como para las actividades que deban desarrollar terceros y que tengan lugar allí. Se deberá tener en cuenta las siguientes medidas:

- Evitar la ejecución de trabajos por parte de terceros sin supervisión;
- Acompañar siempre al personal externo al Organismo cuando se requiera acceder a las áreas seguras;
- Bloquear físicamente e inspeccionar periódicamente las áreas seguras;
- Limitar el acceso a las áreas seguras donde existan instalaciones de procesamiento de información sensible;
- Mantener las áreas seguras cerradas, con llave o mediante bloqueo electrónico de acuerdo al método de control de acceso físico dispuesto;
- Definir un periodo para la revisión y actualización de los derechos de acceso físico a estas áreas;
- Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información;
- Mantener estos recintos ordenados y en buenas condiciones de higiene;
- Controlar diariamente el funcionamiento de los aires acondicionados en aquellos recintos donde sea indispensable su uso;
- Prevenir la instalación de servicios y equipamiento sin previa autorización de personal técnico autorizado;
- Instruir respecto a la conexión de equipamiento con la guía de personal técnico autorizado.

5.2 SEGURIDAD DE LOS EQUIPOS Y PUESTOS DE TRABAJO

Se definirán e implementarán controles que permitan evitar la pérdida, daño, robo o compromiso de los activos físicos informáticos que puedan generar la interrupción de las actividades de la S.R.T., así como proteger el equipo de amenazas físicas y ambientales.

Se deberá establecer un procedimiento para informar y accionar en caso de incidentes relacionados con la pérdida o robo de dispositivos y/o equipamiento de la S.R.T..

Asimismo, se deberá mantener un registro de los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.

Por último, es necesario el mantenimiento interno de todo el entorno edilicio donde se encuentren los activos físicos, particularmente en aquellas áreas seguras identificadas con procesamiento de información crítica.

5.2.1 Emplazamiento y protección de equipos

El equipamiento deberá ser ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, así como las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes aspectos:

- Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y permita un control de acceso adecuado;
- Ubicar las instalaciones de procesamiento y almacenamiento de información que gestionan información sensible en un sitio que permita la supervisión durante su uso;
- Revisar regularmente las condiciones ambientales para verificar que éstas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información;
- Establecer e implementar medidas de protección contra descargas eléctricas que pudieran afectar el equipamiento.

5.2.2 Seguridad del equipamiento fuera de las instalaciones

Se deberá coordinar la adopción de medidas de seguridad para que el equipamiento sea ingresado o retirado del Organismo con una autorización previa y habiéndose adoptado todos los recaudos necesarios.

El equipamiento informático no deberá ser retirado de la sede de la S.R.T. sin una autorización formal. Asimismo, para el uso de estos fuera del ámbito de la S.R.T., se establecerán lineamientos específicos de seguridad en dispositivos móviles y trabajo remoto.

Los riesgos de seguridad al trabajar fuera de las dependencias de la S.R.T. pueden variar entre las diferentes sedes y deben ser tomados en cuenta al momento de establecer las medidas de seguridad.

Por otro lado, se deberá implementar un registro del equipamiento retirado con la previa autorización, indicando su localización física y asignación organizacional y personal para su uso.

En todos los casos, se deben tener en cuenta las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se deberá mantener una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la S.R.T., cuando sea conveniente.

Por último, se deberá concientizar y capacitar a todo el personal de la S.R.T. sobre las medidas de seguridad para el traslado seguro y gestión del equipamiento informático fuera del ámbito del Organismo. Asimismo, es recomendable impulsar medidas tendientes a minimizar los riesgos asociados al traslado de equipamiento teniendo en cuenta los diferentes escenarios que pudieran presentarse en dicho traslado.

5.2.3 Cuidado de puestos de trabajo: bloqueo de sesión

Los equipos informáticos requieren una protección específica contra accesos no autorizados. Por ello se deberán establecer mecanismos de bloqueo que incluyan el cierre de las sesiones activas al finalizar las tareas.

Asimismo, se deberán coordinar tareas de concientización para todo el personal, acerca de los requerimientos, lineamientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

5.2.4 Cuidado de puestos de trabajo: escritorios despejados

Se adoptarán medidas relativas a mantener escritorios limpios con el fin de proteger documentos en papel y dispositivos de almacenamiento removibles que pudieran ser utilizados por personal no autorizado.

Se deberán coordinar tareas de concientización para todo el personal, acerca de los requerimientos, lineamientos y procedimientos de seguridad, para la protección de documentos en papel y dispositivos de almacenamiento removibles, así como de sus funciones en relación a la implementación de dicha protección.

5.3 PROTECCIÓN FRENTE A INTERRUPCIONES

Se deberá realizar un análisis del impacto de eventuales consecuencias ante una interrupción prolongada del procesamiento de dicha información, con el objeto de definir qué componentes son necesarios de abastecer con energía alternativa. Dicho análisis debe ser realizado en función de la criticidad de la información procesada, en el marco del Plan de Continuidad del Organismo.

Asimismo, se deberán establecer medidas para proteger los activos de información frente a la interrupción de sus operaciones, así como interferencias o daños de los cables eléctricos y de la red que transporten datos o apoyen los servicios de información.

5.3.1 Instalaciones de suministro de energía

El equipamiento deberá estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía debe seguir las especificaciones del fabricante o proveedor de cada equipo.

Para asegurar la continuidad del suministro de energía, se deberán contemplar, en la medida de lo posible, las siguientes medidas de control:

- Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía;
- Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la S.R.T.;
- Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía;
- Disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado;
- Inspeccionar y probar periódicamente los generadores para asegurar que funcionen según lo previsto;
- Implementar protección contra descargas eléctricas en los edificios y líneas de comunicaciones externas de acuerdo con las normativas vigentes.

Por otra parte, también se deberá:

- Asegurar, en aquellos casos en que se cuente con generadores cuyo encendido no sea automático, que el funcionamiento de la UPS dure el tiempo necesario para el encendido manual de los generadores;
- Inspeccionar y probar periódicamente los equipos de UPS para asegurar que funcionan correctamente y que tienen la autonomía requerida;

- Mantener actualizado e informar respecto de cualquier cambio en las condiciones de suministro eléctrico requeridas por los sistemas, ya sea en términos de consumo u otros parámetros propios del suministro;
- Contemplar en los planes de contingencia, las acciones que han de emprenderse ante una falla de la UPS.

5.3.2 Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra intercepción o daño. Para ello, se deberán llevar a cabo las siguientes acciones:

- Cumplir con los requisitos técnicos vigentes;
- Utilizar piso ducto o cableado embutido en la pared o bandejas porta cable -siempre que sea posible-, cuando corresponda a las instalaciones de procesamiento de información;
- Proteger el cableado de red contra intercepción no autorizada o daño mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas;
- Separar los cables de energía de los cables de comunicaciones para evitar interferencias;
- Proteger, de ser posible, el tendido del cableado troncal mediante la utilización de ductos blindados.

5.3.3 Mantenimiento de los equipos e instalaciones con impacto en el procesamiento de información critica

Se deberá realizar el mantenimiento de los equipos e instalaciones con impacto en el procesamiento de información crítica (aquellos que garantizan el funcionamiento de los medios de procesamiento de información, como por ejemplo generadores, UPS, aires acondicionados, cableados, etc.) para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor;
- Mantener un listado actualizado del equipamiento con el detalle de la frecuencia con la que se realiza el mantenimiento preventivo;
- Establecer que sólo el personal de mantenimiento autorizado puede brindar ese servicio y llevar a cabo reparaciones en el equipamiento;
- Registrar todas las fallas, ya sean supuestas o reales y todo el mantenimiento preventivo y correctivo realizado;
- Registrar el retiro de equipamiento de la sede de la S.R.T. para su mantenimiento;
- Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66584434-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO VII Seguridad Física y Ambiental-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 8 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:40:07 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:51:26 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:51:28 -03:00